



Área Departamental de Engenharia da Eletrónica e Telecomunicações e de
Computadores (ADEETC)

LEIC

Trabalho prático 3

BGP

Redes de Internet

Semestre de Inverno 2020/2021

Docente: Luís Pires

Grupo 9 LI51N

41462 Hugo Cameira

43602 Cecília Duarte

43755 Luís Guerra

Índice

Introdução	5
Topologia do trabalho	6
Fase 1 – Endereçamento.....	11
1 - Atribuição de endereços IPv4	11
a).....	11
b)	11
c).....	11
d)	11
Fase 2 – OSPFv2, RIPv2, rotas estáticas e redistribuição de rotas	13
1 - Configuração do protocolo OSPF.....	13
a).....	13
b)	15
c).....	15
d)	15
e).....	15
2 - Configuração de rotas estáticas de interligação entre domínios (ISP e alguns clientes)....	15
3 - Configuração do protocolo RIPv2	16
a).....	16
b)	16
4 - Redistribuição de rotas no AS do ISP entre os protocolos de routing IGP	17
a).....	17
b)	17
c).....	17
d)	17
e).....	17
f)	17
g)	17
h)	17
i)	18
Fase 3 – BGPv4, redistribuição de rotas entre o OSPFv2 e o BGP	20
1 - BGPv4 básico	20
a).....	22
b)	22

c).....	22
d)	22
e).....	26
f)	26
g)	26
h)	26
i)	26
j)	27
k)	27
l)	27
m)	27
n)	27
o)	27
p)	28
q)	28
2 – Implementação de políticas no iBGP no ISP	30
a).....	30
b)	30
c).....	30
d)	30
3 – Políticas de eBGP, entre o ISP e os seus clientes.....	31
a).....	32
b)	32
c).....	32
d)	32
4 – Route Refletor (RR)	33
Fase 4 – BGPv4 avançado.....	34
1 - Ligações eBGP de trânsito e <i>peering</i> do ISP	34
2 – Políticas de segurança do ISP relativas aos AS dos <i>tiers</i> superiores.....	35
3 – Políticas de tráfego de saída do ISP	35
a).....	35
Fase 5	36
1 – Rotas internas no ISP	36
a).....	36
b)	36
c).....	36

d)	36
e).....	36
f).....	36
Conclusão	37
Webgrafia.....	37

Introdução

- › Este trabalho tem como objetivo o aprofundamento os conhecimentos sobre o protocolo de encaminhamento BGP¹ e de técnicas de *Policy Based Routing* (PBR), como também outros protocolos de *routing* anteriormente abordados e lecionados em aula: RIPv2, OSPFv2 e rotas estáticas.

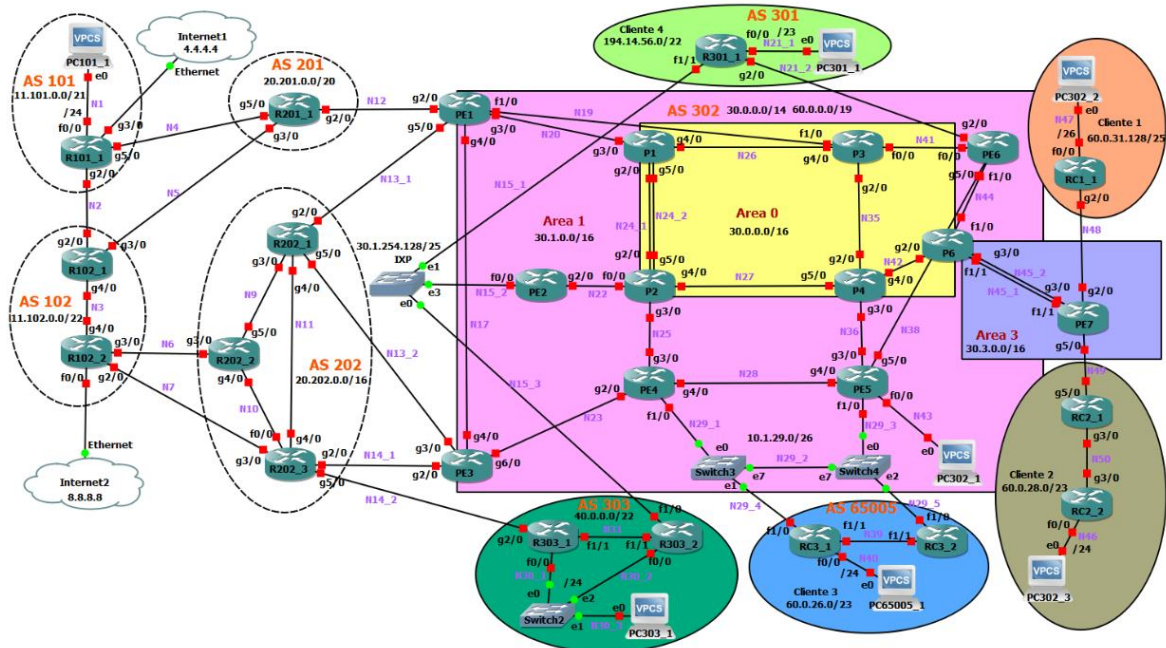
O trabalho divide-se em várias fases:

- › Fase 1 que trata de questões sobre o endereçamento usado na topologia;
- › Fase 2, relacionado com o uso dos protocolos OSPF, RIP, rotas estáticas e redistribuição de rotas;
- › Fase 3 – fase sobre o protocolo BGP (básico) e a distribuição de rotas entre OSPF e BGP;
- › Fase 4 – fase sobre o protocolo BGP (avançado);
- › Fase 5, última fase em que se propõe algumas questões que aprofundam sobre as fases anteriores.

Neste projeto, existe um *Internet Service Provider* (ISP) que tem um Autonomous System (AS) atribuído, o AS 302. Este ISP tem 4 clientes, incluindo um que possui o seu próprio AS privado (Cliente 3) e outro que possui um AS público (Cliente 4). Na topologia apresentada temos ainda mais 5 ASs distintos.

¹ BGP (*Border Gateway Protocol*) é um protocolo baseado em *path-vector* usado para trocar informações entre sistemas autónomos na Internet. Quando usado dentro de um AS (*Autonomous System*) é chamado iBGP, ‘i’ para interior/internal. Quando aplicado na Internet é conhecido como eBGP, ‘e’ para exterior/external.

Topologia do trabalho



A topologia apresentada representa vários sistemas autónomos (AS), em 3 *tiers*, em que o *Internet Service Provider* (ISP) faz parte do *tier 3* e possui o AS 302.

O ISP possui 4 Clientes. Dois fazendo parte do seu AS, um com AS privado e outro com AS público. Apesar de na topologia o ISP ter apenas 4 Clientes, deve ser assumido que o ISP pode ter, ou vir a ter, centenas ou milhares de clientes. No *tier 1* temos os AS 101 e 102. No *tier 2* temos os AS 201 e 202 e no *tier 3* temos os AS 301, 302, 303 e 65005.

Os AS utilizam entre eles o protocolo de *routing* BGPv4. O BGP é um protocolo de encaminhamento usado pela internet para envio de *packets*. O BGP é um EGP².

Os AS do *tier 3* utilizam um *Internet Exchange Point*³ (IXP) para trocarem tráfego entre eles. O objetivo é tentar evitar usar para isso os AS do tier acima aos quais teriam de pagar pelo tráfego que por lá passe.

Quando for necessário usar *Interior Gateway Protocol*⁴ (IGP) deverá ser utilizado o OSPFv2, sendo o Cliente 2 uma exceção dado pretender usar o RIPv2.

² Um EGP é um *Exterior Gateway Protocol*, ou seja, é um protocolo de encaminhamento utilizado para trocar informações entre *gateways* de Sistemas Autónomos diferentes (vizinhos exteriores).

³ “An Internet exchange point (IX or IXP) is the physical infrastructure through which Internet service providers (ISPs) and content delivery networks (CDNs) exchange Internet traffic between their networks (autonomous systems).”, at IXP from Wikipedia.

⁴ *Interior Gateway Protocol* (IGP) é um protocolo de encaminhamento usado dentro (no Interior) de um Sistema Autónomo (AS), criando vizinhos interiores.

Internet Service Provider (ISP)

O ISP⁵ é composto por um domínio OSPFv2, por um domínio/rede (Cliente 1), por um domínio/rede que usa RIPv2 como IGP (Cliente 2). Inclui também como seus clientes o AS 65005 (Cliente 3) e o AS 301 (Cliente 4).

O AS 301 é um cliente com um AS público, o qual usa o ISP como AS de trânsito dado não ter dimensão para se ligar diretamente a um fornecedor do *tier* acima.

Os routers do ISP são designados *Provider* (P) e *Provider Edge*⁶ (PE). Os routers P são routers internos ao AS, neste caso também internos ao domínio OSPFv2 do ISP, os quais não possuem interfaces para o exterior do domínio. Os routers P servem, por exemplo, para interligar locais geograficamente afastados do ISP usando ligações de débito muito elevado. Os routers PE, para além de poderem participar no trânsito interno do ISP, possuem interfaces para ligar a clientes e a outros AS⁷, no caso do OSPFv2 são ASBR.

Preferencialmente o tráfego entre os vários locais do ISP deve passar pelos routers P na área 0 que devem funcionar como um *backbone* no que se refere ao tráfego interno do ISP.

As áreas 0 e 1 do domínio OSPF do ISP são áreas normais. Quanto à área 3 pretende-se que, de preferência, não tenha de lidar com tabelas de *routing* pesadas em termos do suporte do endereçamento relativo a rotas externas ao domínio OSPF do ISP.

Relações com os clientes

As *start-ups*, representadas pelos Clientes 1 e 2, atingiram um nível de crescimento e maturidades tal que se tornaram independentes. Desta forma os seus routers não devem estar no domínio OSPF interno do ISP. Foi realizada a sua separação da rede do ISP e é necessário apoiar a sua migração.

- › O Cliente 1 expressou a sua incapacidade técnica e usará **routing estático**.
- › O Cliente 2 pretende usar como IGP o **RIPv2**.
- › O Cliente 3 pretende usar **BGPv4** como EGP e requereu um AS público. Este não lhe foi atribuído dado não ter dimensão suficiente em termos de número de redes internas. Por isso irá migrar para um AS privado, o AS 65005.
- › O Cliente 4, por ser um cliente com uma rede mais complexa e com um bloco de endereçamento IP antigo/*legacy PI*, apesar de na topologia apresentada neste

⁵ Um ISP é uma “organização” que fornece serviços para aceder, participar, usar na Internet.

⁶ Router entre a área de um ISP e área de outro ISP.

⁷ Um sistema autónomo é uma coleção de prefixos de encaminhamento controlados por apenas uma entidade.

trabalho apenas estar presente parte da sua rede, requisitou também um AS, o qual lhe foi atribuído, o AS 301.

Relações de Trânsito/*Peering*

O AS 302 criou um *Internet Exchange Point* (IXP) para melhorar a qualidade e rentabilizar melhor o uso da Internet entre os AS no mesmo *tier*, ligados ao IXP, criando relações de *peering* entre eles.

O AS 201 informou o ISP que, com a ativação do BGP entre ambos, este poderá usufruir de um plano de trânsito mais favorável em relação à concorrência e poderá, inclusivamente, aceder a todas as redes dos seus *Peers* e *Content Deliver Networks* (CDN) de forma gratuita.

Endereçamento

Os endereços IP para as redes de interligação entre routers, são normalmente disponibilizados pelo AS que está a fornecer trânsito.

De acordo com o RIPE⁸, o qual atribuiu os seguintes blocos IPv4 públicos e AS, e o ISP que decidiu atribuir endereços IP do seu bloco público ao Cliente 3, a distribuição de blocos de endereços IPv4 pelos AS é a seguinte:

- > AS 101: 11.101.0.0/21
- > AS 102: 11.102.0.0/22
- > AS 201: 20.201.0.0/20
- > AS 202: 20.202.0.0/16
- > AS 301 (Cliente 4): 194.14.56.0/22
- > AS 302: 30.0.0.0/14 e 60.0.0.0/19
- > AS 303: 40.0.0.0/22
- > AS 65005 (Cliente 3): “Bloco IPv4 a definir pelo gestor de rede do ISP a partir do bloco do seu bloco (AS 302)”, um/23

A atribuição de endereços IPv4 públicos em cada AS deve respeitar os blocos de endereços IP atribuídos a cada AS pelo RIPE ou delegados pelo respetivo ISP (caso de alguns clientes). Devem ser usados endereços IPv4 privados onde não forem necessários endereços públicos. Por exemplo, redes internas aos AS podem utilizar nas redes *point-to-point* (PTP) endereços privados.

⁸ “RIPE is a forum open to all parties with an interest in the technical development of the Internet. The RIPE community’s objective is to ensure that the administrative and technical coordination necessary to maintain and develop the Internet continues.”, at RIPE from Wikipedia.

O ISP optou por utilizar o bloco 30.0.0.0/14 para as suas redes internas e de interligação com os seus clientes. O bloco 60.0.0.0/19 é usado para delegar endereços IP aos seus clientes. Quando bloco 60.0.0.0/19 esgotar, o ISP passará a delegar aos seus clientes endereços IP do bloco 30.0.0.0/14. Conforme for progredindo em número de clientes a intenção do ISP é aproveitar ambos os blocos de endereçamento.

Os clientes do ISP deverão ter os seguintes endereços públicos disponíveis:

- › Cliente 1, interno ao AS 302: 128 endereços públicos;
- › Cliente 2, interno ao AS 302: 512 endereços públicos;
- › Cliente 3 (AS 65005): 512 endereços públicos, “Bloco IPv4 a definir pelo gestor de rede do ISP a partir do seu bloco (AS 302)”;
- › Cliente 4, AS 301 (194.14.56.0/22): 1024 endereços públicos.

Regras de distribuição de endereços IP

Utilizou-se uma política de nomear as redes por ordem crescente, sempre que possível, de cima para baixo e da esquerda para a direita, segundo a topologia da figura. Existem algumas exceções pontuais na regra do endereçamento como, por exemplo, o caso das interfaces dos routers que servem de *gateways* nas LAN onde existem outros equipamentos e que recebem quase o maior endereço IP da rede a que estão ligados, e o PC o menor endereço disponível.

Se existirem vários routers numa rede recebem endereços no fim do bloco atribuído à LAN com ajustes para ajudar a memória, por exemplo se o bloco vai até... .255, o router 3 fica com o253, o 2 com o .252, etc.

ISP

- › LAN c/ endereço público:
30.área.<nº rede>.m
- › Redes PTP e redes de interligação que usem endereços privados:
10.área.<nº rede>.m

ISP – Clientes

- › Clientes internos ao ISP (os que partilham o bloco IPv4 do ISP)
 - 60.0.<varia, sendo os endereços atribuídos a começar na parte de cima do bloco do ISP>.m
 - Numa LAN com DC ou PC, os routers possuem dos últimos endereços IP e os DC ou PC o menor disponível.

AS

- > Redes PTP e redes de interligação entre AS:
N.<nº AS menor>.<nº rede>.m (N depende do bloco IP do AS)
- > Redes PTP e redes de interligação que usem endereços privados:
10.<nº AS>.<nº rede>.m

A ligação ao IXP usa endereços IPv4 públicos cedidos pelo AS 302.

Fase 1 – Endereçamento

1 - Atribuição de endereços IPv4

Cada AS tem redes que necessitam de endereços IPv4 públicos, por exemplo onde se situarem servidores de DNS, Web, email, etc., outras em que os endereços podem ser privados (redes internas onde o uso de NAT pode permitir poupar endereços IPv4 públicos e continuar a manter comunicação com o resto do mundo).

Assuma que cada AS é gerido por uma entidade distinta dos outros AS. Os equipamentos de rede de um AS só devem ser acedidos remotamente para gestão a partir de dentro do respetivo AS.

a)

Para efeitos de sumarização de rotas por parte dos ABRs é preferível ter endereços de IP estruturados de modo a se alinharem com as diversas áreas de OSPF. Uma maneira para fazer isso seria alocar blocos de endereços de IP distintos para cada área.

b)

Com a distribuição apresentada, que permite a existência de vários endereços para cada cliente, é bastante provável que, numa rede real, pudesse ocorrer uma falta de endereços IPv4 para outros blocos. A má distribuição é causada principalmente pela alocação de mais endereços do que aqueles que são necessários a cada cliente e pela ineficiência de *subnetting*. Devido aos efeitos de *subnetting* é difícil de usar todos os endereços alocados para um bloco.

Este tipo de uso de endereços de IP públicos pode não trazer nenhum problema no exemplo de topologia deste trabalho, mas numa escala maior, em termos mais realistas, pode deixar de ser eficiente. Este tipo de distribuição pode causar *IP address exhaustion* ou *depletion*. Uma boa técnica para mitigar este problema seria o uso de NAT⁹ mas esta opção foi ignorada para simplificar.

c)

Para que não seja possível o acesso e controlo dos equipamentos do ISP, ou outro AS, fora do próprio AS, uma solução passaria por tornar os endereços dos routers internos e ABRs privados, para que não possam ser acedidos por equipamentos no exterior do AS. Os ASBRs desse AS teriam de ter interfaces públicas para efetuar a comunicação com o exterior do AS. Isto significa então que teríamos de alocar endereços privados ao AS em questão, aos seus routers internos, ABRs e também às interfaces que comunicam com o interior do AS do router ASBR.

d)

Endereços de IP públicos são vantajosos se for necessário aceder à Internet, estes ficam acessíveis a outros dispositivos através da Internet enquanto que nos endereços privados isso não acontece. Porém isto traz problemas de segurança devido a esses endereços públicos ficarem acessíveis a todos, pode vir a trazer problemas na rede se nenhuma medida adicional de proteção for aplicada. Ou seja, neste aspeto um endereço privado parece mais seguro e menos problemático a fatores externos que a sua própria rede não poderia prever. Apesar dessa vantagem isto traz também o outro lado da moeda, o

⁹ NAT – *Network Address Translation*, permite a um ISP mascarar blocos de endereços privados da rede com apenas um endereço de IPv4 público em vez de alocar um endereço público para cada dispositivo da rede.

isolamento. Não estando exposto a outras máquinas, a outras redes, não há nenhuma maneira de se fazer comunicação entre redes com endereços privados. Se for necessário esse tipo de ligação e troca de informação com outros sistemas, não será possível com o uso de endereços privados.

Fase 2 – OSPFv2, RIPv2, rotas estáticas e redistribuição de rotas

1 - Configuração do protocolo OSPF

Nas tabelas de encaminhamento dos routers do OSPF constam todas as rotas dos respetivos domínios. Para verificar a correta ligação entre estes dispositivos do ISP foi feito um ping via TCLSH a partir do router PE6.

```
PE6(tcl)#foreach address {  
+>30.1.255.1  
+>30.1.255.2  
+>30.1.255.3  
+>30.1.255.4  
+>30.1.255.5  
+>30.1.255.6  
+>30.3.255.7  
+>10.0.255.1  
+>10.0.255.2  
+>10.0.255.3  
+>10.0.255.4  
+>10.0.255.6  
+>30.1.43.1  
+>} { ping $address}
```

Figura 1 - Ping em PE6

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 30.1.255.1, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 80/132/168 ms  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 30.1.255.2, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 88/126/160 ms  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 30.1.255.3, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 68/91/108 ms  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 30.1.255.4, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/45/68 ms  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 30.1.255.5, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/36/44 ms  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 30.1.255.6, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 30.3.255.7, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/62/128 ms  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 10.0.255.1, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 88/132/164 ms  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 10.0.255.2, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 64/76/88 ms  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 10.0.255.3, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/34/68 ms  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 10.0.255.4, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/56/92 ms  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 10.0.255.6, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/34/56 ms  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 30.1.43.1, timeout is 2 seconds:  
!!!!  
Success rate is 80 percent (4/5), round-trip min/avg/max = 36/43/48 ms  
PE6(tcl)#
```

Figura 2 - Resultado do ping

a)

Um *designated* router¹⁰ (DR) deve ser atribuído por cada *network*, ou seja, cada segmento/link (*broadcast/non-broadcast link*).

Para eleger um DR iremos recorrer ao algoritmo cuja primeira regra (e primeira prioridade) é a prioridade do router e segunda regra para desempatar as prioridades dos routers caso sejam iguais, o maior router ID.

Foi decidido no final que os routers PE1, PE4 e PE6 seriam os melhores routers para serem *designated* routers sendo que foram mudados os tipo de network (antes era *point-to-point*) nas ligações entre estes routers e os seus vizinhos adjacentes.

No AS 303, o R303_2 é o DR e o R303_1 é o BDR no processo 303 de OSPF. No AS 102, o router R102_2 é o DR.

Como foi utilizada a configuração já dada não foi necessário ter que fazer muitas alterações, só mesmo para criar eleição de *designated* routers retirando o tipo de *network point-to-point* nos segmentos necessários. Cada router do processo OSPF no ISP faz *advertisement* das redes das suas interfaces para que possa haver comunicação total entre as áreas.

¹⁰ *Designated routers* permitem reduzir o número de adjacências numa rede conseguindo deste modo reduzir também a quantidade de tráfego.

Abaixo estão apresentadas algumas configurações do processo 1 OSPF nos routers PE1, PE2, P1, P6 e PE7.

```
router ospf 1
log-adjacency-changes
auto-cost reference-bandwidth 10000
redistribute bgp 302 subnets
passive-interface default
no passive-interface GigabitEthernet2/0
network 10.1.22.0 0.0.0.3 area 1
network 30.1.254.128 0.0.0.127 area 1
network 30.1.255.2 0.0.0.0 area 1
```

Figura 5 - OSPF PE2

```
router ospf 1
log-adjacency-changes
auto-cost reference-bandwidth 10000
redistribute bgp 302 subnets
passive-interface default
no passive-interface FastEthernet1/0
no passive-interface GigabitEthernet3/0
no passive-interface GigabitEthernet4/0
network 10.1.17.0 0.0.0.3 area 1
network 10.1.19.0 0.0.0.3 area 1
network 10.1.20.0 0.0.0.3 area 1
network 30.1.255.1 0.0.0.0 area 1
default-information originate
```

Figura 3 - OSPF PE1

```
router ospf 1
log-adjacency-changes
auto-cost reference-bandwidth 10000
area 3 nssa
redistribute static subnets
redistribute rip subnets
passive-interface default
no passive-interface FastEthernet1/1
no passive-interface GigabitEthernet3/0
network 10.3.49.0 0.0.0.3 area 3
network 10.3.145.0 0.0.0.3 area 3
network 10.3.245.0 0.0.0.3 area 3
network 30.3.48.0 0.0.0.3 area 3
network 30.3.255.7 0.0.0.0 area 3
```

Figura 4 – OSPF PE7

```
router ospf 1
log-adjacency-changes
auto-cost reference-bandwidth 10000
area 3 nssa default-information-originate
passive-interface default
no passive-interface FastEthernet1/0
no passive-interface FastEthernet1/1
no passive-interface GigabitEthernet2/0
no passive-interface GigabitEthernet3/0
network 10.0.42.0 0.0.0.3 area 0
network 10.0.255.6 0.0.0.0 area 0
network 10.1.44.0 0.0.0.3 area 1
network 10.3.145.0 0.0.0.3 area 3
network 10.3.245.0 0.0.0.3 area 3
```

Figura 6 - OSPF P6

```
router ospf 1
log-adjacency-changes
auto-cost reference-bandwidth 10000
passive-interface default
no passive-interface GigabitEthernet2/0
no passive-interface GigabitEthernet3/0
no passive-interface GigabitEthernet4/0
no passive-interface GigabitEthernet5/0
network 10.0.26.0 0.0.0.3 area 0
network 10.0.241.0 0.0.0.3 area 0
network 10.0.242.0 0.0.0.3 area 0
network 10.0.255.1 0.0.0.0 area 0
network 10.1.20.0 0.0.0.3 area 1
```

Figura 6 - OSPF P1

b)

Os tipos de LSA que andam na área 3 são do tipo 1, Router LSA, do tipo 3 – Summary LSA e do tipo 7 (a área 3 é NSSA logo recebe LSAs externos em LSAs do tipo 7 em vez do tipo 5). Podemos confirmar esta resposta com o comando **sh ip ospf database**.

c)

Em OSPF a melhor rota é escolhida pelo a métrica custo, o menor valor é a melhor opção logo para manter a preferência poder-se-ia alterar o custo de N17 para menor ou aumentar o custo da rota paralela.

d)

Podemos verificar na configuração do router PE1 e no router PE3 que na interface G4/0 que os liga foi executado o comando **ip ospf cost** – este comando altera o custo do segmento. O valor foi alterado de *default* para 5. Quando fazemos **sh ip route** podemos ver o custo acumulativo de enviar pacotes por cada rota apresentada (em OSPF). Este custo, para os endereços no enunciado, vai ser 6 devido ao custo do link usado para a ligação entre estes routers. O *link* tem uma *bandwith* superior a 100 Mbs logo o seu custo vai ser 1, no final o custo acumulado será $5 + 1 + 6$.

e)

Para fazer balanceamento de carga em OSPF por estes routers alteramos a métrica, *route cost*, para serem iguais em ambos os routers em questão para que o tráfego seja distribuído pelos dois. Para manipular a métrica custo usamos o comando **ip ospf cost <value>**.

2 - Configuração de rotas estáticas de interligação entre domínios (ISP e alguns clientes)

Rotas estáticas são definidas com o comando **ip route 0.0.0.0 0.0.0.0 30.3.48.2**, este comando define a rota estática de RC1_1, consequentemente existe também rota estática em PE7. Neste caso é necessário devido à especificação do Cliente 1. Esta rota não é propagada, apenas se verifica nos routers RC1_1 e PE7.

```
PE7#ping 60.0.31.251
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 60.0.31.251, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/12/16 ms
```

Figura 7 - Ping de PE7 para RC1_1

```
RC1_1#ping 30.3.255.7
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 30.3.255.7, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/60/64 ms
```

Figura 8 - Ping de RC1_1 para PE7

Rota estática definida em RC1_1:

```
S* 0.0.0.0/0 [1/0] via 30.3.48.2
```

Rota estática definida em PE7:

```
S 60.0.31.128 [1/0] via 30.3.48.1
```

Existem também outras rotas estáticas definidas por outros routers nos diferentes sistemas autônomos. Abaixo são apresentadas essas rotas.

Sistema Autônomo (AS)	Router	Rota Estática
65005	Todos	60.0.26.0 255.255.254.0
101	RC101_1	11.101.0.0 255.255.248.0
102	Todos	11.102.0.0 255.255.252.0
202	Todos	20.202.0.0 255.255.0.0
201	RC201_1	20.201.0.0 255.255.240.0
302	Todos	30.0.0.0 255.252.0.0 60.0.0.0 255.255.224.0
301	RC301_1	194.14.56.0 255.255.254.0
303	Todos	40.0.0.0 255.255.252.0

Estas rotas são específicas devido ao comando **network** executado na configuração de cada BGP nestes routers. Para o endereço especificado em **network** aparecer na tabela de encaminhamento é necessário fazer **ip route**, criar a rota estática para esse endereço que se quer anunciar.

3 - Configuração do protocolo RIPv2

a)

Para não serem enviadas mensagens RIP usa-se o comando **passive-interface <interface>** na configuração das interfaces que vão ligar a dispositivos que não têm interesse.

b)

Como é dito no enunciado o Cliente 2 expandiu-se e ficou independente por isso deve ser necessário algum mecanismo de segurança para as suas tabelas de encaminhamento, algo que o RIPv1 não suporta. Existem outros fatores que impedem o uso da versão 1 de RIP como a sumarização de rotas.

4 - Redistribuição de rotas no AS do ISP entre os protocolos de routing IGP

a)

Para este caso, não há necessidade de contabilizar custos internos (existência de várias ligações) porque só temos uma rota, aspecto principal no custo E1. Por isso, é mais vantajoso usar o custo E2 mantendo o custo igual aquando da redistribuição.

b)

As rotas OSPF não são distribuídas pelo RIP pois as redes anunciadas pelo protocolo RIP em vigor no Cliente 2 já têm acesso às redes do processo OSPF (devido ao router PE7 que faz parte do RIP e do processo OSPF do ISP). Ou seja, não foi necessária fazer *mutual distribution*. Também no router PE7 é configurada a rota estática para acesso ao cliente 1, deste modo forçando esse endereço nas tabelas de encaminhamento do processo de OSPF 1 (podendo haver assim comunicação com o cliente 1 que usa *routing* estático).

c)

Se os routers do ISP que utilizam OSPF poderem ter acesso às rotas do cliente 1, que usa *routing* estático, e do cliente 2 que usa o protocolo RIP é necessário que o router PE7 que está na fronteira entre o cliente 2 e a área 3 do ISP anuncie essas rotas que PE7 recebe.

d)

Sim, poderia ser uma rede com endereços privados pois estamos a falar duma ligação a um cliente, e que não está ligado diretamente à Internet.

e)

Não, esta rota é derivada pelo protocolo RIP.

f)

O comando **ip ospf network point-to-point** classifica a ligação nessa interface com outro router como *point-to-point*, o que faz com que a prioridade do router passe a 0 e deixe de haver eleição de DR/BDR. Ou seja, se isto for removido a prioridade passa ao valor *default* que é 1 e inicia-se o processo de eleição de DR/BRD com os seus vizinhos.

g)

Os comandos **network** apresentados são necessárias para anunciar essas redes na área 0 do processo OSPF, para os outros routers em OSPF conseguirem comunicar. Cada comando contém um endereço de interface do router em questão que quer partilhar esses endereços com os seus vizinhos e colocarem nas suas tabelas de *routing* (a *wildmask* serve para mostrar quais os bits que têm de dar “*match*” na eventualidade de um *ping* a um endereço específico por exemplo).

h)

O comando **area 3 nssa** é executado em todos os routers da área 3 para tornar essa área numa *Not-So-Stubby Area* (NSSA). As *keywords* **default-information-originate** são instruídas no ABR da área em questão e forçam o router a gerar uma rota *default*.

Se este comando não for efetuado e houver algum *packet* a ser encaminhado cujo destino não se encontre na tabela de *routing* não vai haver nenhuma *default route* que “dê conta” desse pacote, senão não será possível realizar a operação.

i)

Na área 3 temos o router PE7 que é um ASBR e o P6 que também é um ASBR e um ABR que transforma os LSA tipo 5 recebidos em LSA tipo 7 devido ao tipo de área. Se a área for configurada como *Totally Stubby* o P6 vai deixar de ser ASBR pois não é permitido isto, conseqüentemente vão deixar de circular na área 3 LSAs do tipo 3 (*Summary*). Experimentalmente o que podemos verificar é que os routers das restantes áreas vão deixar de conseguir comunicar com os clientes. Isto porque os routers que estão ligados a estes clientes, os routers da área 3, deixaram de receber os prefixos das outras áreas. Logo, mudar o tipo de área para *Totally Stub* não é uma opção viável.

Quando mudamos o tipo de *stub* na área 3, a resposta de *ping* entre PE1 e o cliente 2 é que não consegue chegar ao destino.

```
PE1#ping 60.0.28.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 60.0.28.1, timeout is 2 seconds:
UUUUU
Success rate is 0 percent (0/5)
```

Figura 9 - Destination Unreachable

Para os routers do AS do ISP conseguir comunicar com ambos os clientes da topologia, e comunicarem entre si, foram feitas as configurações¹¹ seguintes. Para exemplo de configuração foram verificados os routers PE1, P4, PE7 e RC2_1.

O router PE7 tem dois protocolos a funcionar, no OSPF trata de anunciar as rotas das suas interfaces para os outros routers e no protocolo RIP descreve as rotas que quer anunciar, como também tem uma rota *default*.

```
router ospf 1
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 area 3 nssa
 redistribute static subnets
 redistribute rip subnets
 passive-interface default
 no passive-interface FastEthernet1/1
 no passive-interface GigabitEthernet3/0
 network 10.3.49.0 0.0.0.3 area 3
 network 10.3.145.0 0.0.0.3 area 3
 network 10.3.245.0 0.0.0.3 area 3
 network 30.3.48.0 0.0.0.3 area 3
 network 30.3.255.7 0.0.0.0 area 3
!
router rip
 version 2
 passive-interface default
 no passive-interface GigabitEthernet5/0
 network 10.0.0.0
 network 60.0.0.0
 default-information originate
 no auto-summary
!
ip forward-protocol nd
ip route 60.0.31.128 255.255.255.128 30.3.48.1
```

Figura 10 - Configuração PE7

O router PE1 é um router importante pois é um ASBR que liga o ISP a outros ASs da topologia. A configuração do OSPF é a apresentada à direita.

```
router ospf 1
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 redistribute bgp 302 subnets
 passive-interface default
 no passive-interface FastEthernet1/0
 no passive-interface GigabitEthernet3/0
 no passive-interface GigabitEthernet4/0
 network 10.1.17.0 0.0.0.3 area 1
 network 10.1.19.0 0.0.0.3 area 1
 network 10.1.20.0 0.0.0.3 area 1
 network 30.1.255.1 0.0.0.0 area 1
 default-information originate
```

Figura 11 - Configuração OSPF PE1

¹¹ Foram usadas as configurações base já dadas.

São anunciados os endereços de interface para serem divulgados pelo processo OSPF, as interfaces G3/0, G4/0 e F1/0 são configuradas como não-passivas, ou seja, para que estas interfaces possam ser *advertised* (anunciadas). Também é gerada uma rota *default*.

Para o router P4 que é compartilhado pela área 0 (backbone) e área 1, a configuração é muito semelhante à do PE1 como à dos outros routers vizinhos excetuando os endereços das interfaces que vai anunciar na sua configuração.

```
router ospf 1
log-adjacency-changes
auto-cost reference-bandwidth 10000
passive-interface default
no passive-interface GigabitEthernet2/0
no passive-interface GigabitEthernet3/0
no passive-interface GigabitEthernet4/0
no passive-interface GigabitEthernet5/0
network 10.0.27.0 0.0.0.3 area 0
network 10.0.35.0 0.0.0.3 area 0
network 10.0.42.0 0.0.0.3 area 0
network 10.0.255.4 0.0.0.0 area 0
network 10.1.36.0 0.0.0.3 area 1
```

Figura 12 - Configuração P4

O Cliente 2 como especificado no enunciado vai utilizar um protocolo de encaminhamento diferente, vai usar RIP. O PE7 também partilha deste RIP e vai partilhar as rotas do cliente 2 para o ISP. A configuração RIP do Cliente 2 é a seguinte (é usado o router RC2_1).

```
router rip
version 2
network 10.0.0.0
network 60.0.0.0
no auto-summary
```

Figura 13 - Configuração RIP no RC2_1

Para verificar a conexão entre o ISP e os clientes efetuamos um *ping* entre, por exemplo, o PE1 da área 1 e os PCs de cada cliente (1 e 2).

```
PE1#ping 60.0.31.129

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 60.0.31.129, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 208/241/304 ms
```

Figura 14 - Ping entre PE1 e Cliente 1

```
PE1#ping 60.0.28.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 60.0.28.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 216/285/400 ms
```

Figura 15 - Ping entre PE1 e Cliente 2

Fase 3 – BGPv4, redistribuição de rotas entre o OSPFv2 e o BGP

1 - BGPv4 básico

Foi necessário fazer algumas alterações na configuração base, nomeadamente no processo OSPF 202 que continha alguns comandos **network** que não estavam corretos. Essa alteração foi feita no router R202_1 – mudança de processo 1 para 202, no router 202_2 e 202_3 em 2 comandos **network**.

```
R202_2(config)#router ospf 202
R202_2(config-router)#no network 10.0.9.0 0.0.0.3 area 0
R202_2(config-router)#network 10.202.9.0 0.0.0.3 area 0
R202_2(config-router)#no network 10.0.9.0 0.0.0.3 area 0
*Feb 19 16:08:14.283: %OSPF-5-ADJCHG: Process 202, Nbr 20.
ne
R202_2(config-router)#network 10.0.10.0 0.0.0.3 area 0
R202_2(config-router)#network 10.202.10.0 0.0.0.3 area 0
```

Figura 17 - Alteração no R202_2

```
R202_3(config)#router ospf 202
R202_3(config-router)#no network 10.0.10.0 0.0.0.3 area 0
R202_3(config-router)#network 10.202.10.0 0.0.0.3 area 0
R202_3(config-router)#no network 10.0.10.0 0.0.0.3 area 0
*Feb 19 16:09:43.359: %OSPF-5-ADJCHG: Process 202, Nbr 20.2
R202_3(config-router)#no network 10.0.11.0 0.0.0.3 area 0
R202_3(config-router)#network 10.202.11.0 0.0.0.3 area 0
```

Figura 16 - Alteração no R202_3

AS 302 - ISP

- No ISP o BGP que corre é o 302 e em cada router com endereço público é configurado este protocolo, configurando cada *peer*. Por exemplo no PE1 é deste modo:

Todos os vizinhos OSPF estão configurados¹² como *peers* BGP 302 e as ligações exteriores, como para o router no AS 201 e AS 202, também são *peers* para configurar o eBGP.

O comando **neighbor <ip-address> update-source Loopback0** indica que o PE1 irá comunicar com este vizinho pela interface *Loopback0*.

```
router bgp 302
  bgp log-neighbor-changes
  neighbor 20.201.12.1 remote-as 201
  neighbor 20.202.131.1 remote-as 202
  neighbor 30.1.255.2 remote-as 302
  neighbor 30.1.255.2 update-source Loopback0
  neighbor 30.1.255.3 remote-as 302
  neighbor 30.1.255.3 update-source Loopback0
  neighbor 30.1.255.4 remote-as 302
  neighbor 30.1.255.4 update-source Loopback0
  neighbor 30.1.255.5 remote-as 302
  neighbor 30.1.255.5 update-source Loopback0
  neighbor 30.1.255.6 remote-as 302
  neighbor 30.1.255.6 update-source Loopback0
```

Figura 18 - Configuração BGP no PE1

AS 101

- Neste sistema autónomo de *Tier 1* existe apenas um router e um PC. Esse router vai configurar o BGP 101 da seguinte maneira:

Este router tem ligações físicas ao router R102_1 e R201_1. Logo vai ser configurado como BGP *peer* essas ligações. Também vai ter uma ligação direta à Internet simulada por 4.4.4.4 e vai anunciá-lo.

```
router bgp 101
  no synchronization
  bgp log-neighbor-changes
  network 4.4.4.4 mask 255.255.255.255
  network 11.101.0.0 mask 255.255.248.0
  neighbor 11.101.2.2 remote-as 102
  neighbor 11.101.4.2 remote-as 201
  no auto-summary
```

Figura 19 - Configuração BGP no R101_1

¹² Para identificar um vizinho eBGP é necessário indicar o seu endereço e o AS a que pertence com o comando **neighbor <ip-address> remote-as <AS number>**.

AS 102

- O outro AS do *Tier 1*, o AS 102, tem dois routers. Ambos configuram o BGP 102 e configuram este protocolo de modo semelhante. O router R102_1 está ligado ao router do AS 101 e ao router do AS 201, logo este vai tê-los com *peers* na sua configuração. O router R102_2 tem uma ligação direta à Internet simulado por 8.8.8.8 e vai anunciá-la aos seus *peers*.

Também tem duas ligações ao AS 202, ao router R202_2 e R202_3.

```
router bgp 102
no synchronization
bgp log-neighbor-changes
network 11.102.0.0 mask 255.255.252.0
neighbor 11.101.2.1 remote-as 101
neighbor 11.102.3.252 remote-as 102
neighbor 11.102.3.252 update-source Loopback0
neighbor 11.102.3.252 next-hop-self
neighbor 11.102.5.2 remote-as 201
no auto-summary
```

Figura 20 - Configuração BGP do R102_1

- Estes routers vão também configurar um protocolo interno, o OSPF processo 102. Nesta configuração vai haver redistribuição das *subnets* BGP e *advertisement* de cada endereço de interface pertence a cada router.

```
router ospf 102
log-adjacency-changes
auto-cost reference-bandwidth 1000
redistribute bgp 102 subnets
passive-interface default
no passive-interface GigabitEthernet4/0
network 10.0.0.0 0.255.255.255 area 0
network 11.101.2.0 0.0.0.3 area 0
network 11.102.3.0 0.0.0.3 area 0
network 11.102.3.251 0.0.0.0 area 0
network 11.102.0.0 0.0.3.255 area 0
```

Figura 21 - Configuração OSPF do R102_1

AS 202

- Este sistema autónomo é o único do *Tier 2* e fazem parte dele 3 routers.
 - O router R202_1 tem ligações físicas a todos os seus vizinhos OSPF 202 e duas ligações ao ISP nos routers PE1 e PE3.
 - O router R202_2 tem apenas uma ligação exterior ao AS 202, pela interface g3/0 que se liga ao router R102_2 do AS 102.
 - O R202_3 tem os seus vizinhos do AS 202 como também como *peers* os routers a que está ligado, nomeadamente, o router R102_2 do AS 202, o PE3 do AS 302 e o R303_1 do AS 303.
- Na configuração OSPF 202 são redistribuídas as subnets BGP e anunciados endereços de cada interface dos routers interiores ao AS. Na configuração BGP 202 são identificados os vizinhos a que cada router se liga. Por exemplo no router R202_3 as configurações são deste modo:

```
router ospf 202
log-adjacency-changes
auto-cost reference-bandwidth 1000
redistribute bgp 202 subnets
passive-interface default
no passive-interface FastEthernet0/0
no passive-interface GigabitEthernet4/0
network 10.202.10.0 0.0.0.3 area 0
network 10.202.11.0 0.0.0.3 area 0
network 11.102.7.0 0.0.0.3 area 0
network 20.202.255.253 0.0.0.0 area 0
!
router bgp 202
bgp log-neighbor-changes
neighbor 11.102.7.1 remote-as 102
neighbor 11.202.255.251 remote-as 202
neighbor 11.202.255.252 remote-as 202
neighbor 20.202.141.2 remote-as 302
neighbor 20.202.142.2 remote-as 303
```

Figura 22 - Configuração do R202_3

a)

O endereço de IP de origem de uma mensagem BGP de um router é o IP desse mesmo router, se tiver uma interface de *Loopback0* o endereço é o endereço associado a essa interface. Usando interfaces de *Loopback* é possível resolver o problema de existir mais de um caminho para um router e uma interface física “morrer” visto que a sessão BGP não acaba.

b)

Antes dum router anunciar a rota, este vai verificar se o *next-hop* recebido consta na tabela de encaminhamento. Se isso não se verificar esta rota vai ser descartada.

c)

Este comando – **bgp default ipv4-unicast** – serve para desativar o comportamento normal de BGP de anunciar apenas as rotas IPv4 *unicast*, permitindo assim mais protocolos.

d)

É necessário que o iBGP esteja em todos os routers do ISP que corram BGP. Isto porque, as ligações BGP são *full-mesh*, ou seja, todos os routers que corram BGP estão ligados entre si.

Para verificar a comunicação entre os ASs previamente mencionados e configurados foram realizados alguns pings entre os vários routers com endereços públicos.

```
R101_1#ping 20.201.15.251
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.201.15.251, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 64/85/108 ms
```

Figura 23 - Ping entre AS 101 e AS 201

```
R102_1#ping 20.202.255.253
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.202.255.253, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/71/100 ms
R102_1#ping 20.202.255.251
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.202.255.251, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 64/104/144 ms
```

Figura 24 - Ping entre AS 102 e AS 202

```
R101_1#ping 11.102.3.252
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11.102.3.252, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 64/85/108 ms
```

Figura 25 - Ping entre AS 101 e AS 102

```
R101_1#ping 30.1.255.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 30.1.255.3, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 112/203/312 ms
R101_1#ping 30.1.255.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 30.1.255.4, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 140/168/184 ms
```

Figura 26 - Ping entre AS 101 a AS 302

```
PE1#ping 11.101.1.251
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11.101.1.251, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/95/228 ms
PE1#
PE1#ping 11.102.3.252
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11.102.3.252, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 68/103/136 ms
PE1#
PE1#ping 20.202.255.253
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.202.255.253, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/60/128 ms
```

Figura 27 - Ping entre AS 302 e restantes ASs

```

R102_2#ping 11.101.1.251
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11.101.1.251, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/80/144 ms

```

Figura 28 - Ping entre AS 102 e AS 101

```

R201_1#ping 30.1.255.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 30.1.255.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/74/104 ms
R201_1#ping 30.1.255.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 30.1.255.4, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 68/109/148 ms
R201_1#ping 30.1.255.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 30.1.255.6, timeout is 2 seconds:
!!!!

```

Figura 29 - Ping entre AS 201 e AS 302

AS 301

- Existe apenas um router (e um PC) neste sistema autônomo. Neste router é configurado o eBGP 301 da seguinte maneira:
- Como este router se encontra ligado ao IXP também tem acesso ao AS 303 do mesmo Tier e também tem acesso por duas interfaces diferentes ao ISP. Por isso na configuração estas ligações são registradas como *peers* no seus respectivos ASs.

```

router bgp 301
no synchronization
bgp log-neighbor-changes
network 194.14.56.0 mask 255.255.254.0
network 194.14.59.251 mask 255.255.255.255
neighbor 30.1.212.2 remote-as 302
neighbor 30.1.254.132 remote-as 302
neighbor 30.1.254.133 remote-as 303
no auto-summary

```

Figura 30 - Configuração BGP 301

AS 303

- No AS 303 existem dois routers e um PC. O protocolo interno utilizado é OSPF, sendo o processo OSPF 303. Cada um dos routers vai redistribuir as *subnets* do BGP 303 que configurou e os endereços das suas interfaces ligadas.

```

router ospf 303
log-adjacency-changes
auto-cost reference-bandwidth 1000
redistribute bgp 303 subnets
passive-interface default
no passive-interface FastEthernet0/0
no passive-interface FastEthernet1/1
network 10.0.31.0 0.0.0.3 area 0
network 20.202.142.0 0.0.0.3 area 0
network 40.0.0.0 0.0.0.255 area 0
network 40.0.3.251 0.0.0.0 area 0

```

Figura 31 - Configuração OSPF no R303_1

- No exemplo do router R303_1 que tem uma ligação exterior com o router R202_3 do AS 202 vai existir uma relação de *peering* com esse router evidenciado pela configuração do BGP 303.

```

router bgp 303
no synchronization
bgp log-neighbor-changes
network 40.0.0.0 mask 255.255.252.0
neighbor 20.202.142.1 remote-as 202
neighbor 40.0.3.252 remote-as 303
neighbor 40.0.3.252 update-source Loopback0
neighbor 40.0.3.252 next-hop-self
no auto-summary

```

Figura 32 - Configuração BGP no R303_1

AS 65005 – Cliente 3

- No AS 65005 existem dois routers e um PC. O protocolo interno utilizado é OSPF, sendo o processo OSPF 3. Cada um dos routers vai redistribuir as *subnets* do BGP 65005 que configurou e os endereços das suas interfaces ligadas.

```
router ospf 3
log-adjacency-changes
auto-cost reference-bandwidth 1000
redistribute bgp 65005 subnets
passive-interface default
no passive-interface FastEthernet0/0
no passive-interface FastEthernet1/0
no passive-interface FastEthernet1/1
network 10.0.39.0 0.0.0.3 area 0
network 10.1.29.0 0.0.0.63 area 0
network 60.0.26.0 0.0.0.255 area 0
network 60.0.27.251 0.0.0.0 area 0
```

Figura 33 - Configuração OSPF 3

- No exemplo do router RC3_1 que tem uma ligação exterior com os *switches* do AS 202 vão existir vizinhos BGP através dessas ligações, evidenciado pela configuração do BGP 65005.

```
router bgp 65005
no synchronization
bgp log-neighbor-changes
network 60.0.26.0 mask 255.255.254.0
neighbor 10.1.29.1 remote-as 302
neighbor 10.1.29.3 remote-as 302
no auto-summary
!
ip forward-protocol nd
ip route 60.0.26.0 255.255.254.0 Null0 250
```

Figura 34 - Configuração BGP 65005

Para verificar a comunicação estabelecida entre estes ASs configuradas acima foram executados alguns *pings* entre os vários routers.

```
R101_1#ping 60.0.27.252
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 60.0.27.252, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 136/165/180 ms
R101_1#ping 40.0.3.251
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 40.0.3.251, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 88/117/156 ms
R101_1#ping 194.14.59.251
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 194.14.59.251, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 180/244/344 ms
```

Figura 35 - Pings entre AS 101 e AS 301, 303 e Cliente 3

```
R301_1#ping 11.101.1.251
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11.101.1.251, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 164/283/528 ms
R301_1#
R301_1#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 168/246/292 ms
R301_1#ping 20.202.255.253
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.202.255.253, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 124/153/176 ms
R301_1#
R301_1#ping 40.0.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 40.0.0.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R301_1#ping 40.0.3.251
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 40.0.3.251, timeout is 2 seconds:
!!!!!!
```

```
R301_1#ping 30.1.255.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 30.1.255.4, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/90/136 ms
R301_1#
R301_1#ping 11.102.3.252
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11.102.3.252, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 168/216/284 ms
R301_1#ping 11.101.1.251
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11.101.1.251, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 168/200/220 ms
R301_1#ping 20.202.255.252
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.202.255.252, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 160/200/248 ms
```

Figuras - Ping entre AS 301 e ASs do Tier 1, Tier 2 e Tier 3.


```

RC3_2#ping
Protocol [ip]:
Target IP address: 11.101.1.251
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 60.0.27.252
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11.101.1.251, timeout is 2 seconds:
Packet sent with a source address of 60.0.27.252
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 108/161/228 ms
RC3_2#
RC3_2#ping
Protocol [ip]:
Target IP address: 11.102.3.252
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 60.0.27.252
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11.102.3.252, timeout is 2 seconds:
Packet sent with a source address of 60.0.27.252
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 152/218/252 ms
RC3_2#
RC3_2#ping
Protocol [ip]:
Target IP address: 20.201.15.251
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 60.0.27.252
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.201.15.251, timeout is 2 seconds:
Packet sent with a source address of 60.0.27.252
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 116/144/180 ms

```

```

RC3_2#ping
Protocol [ip]:
Target IP address: 194.14.59.251
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 60.0.27.252
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 194.14.59.251, timeout is 2 seconds:
Packet sent with a source address of 60.0.27.252
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 96/120/164 ms

```

Figuras - Pings entre Cliente 3 e os outros ASs

```

RC3_2#ping
Protocol [ip]:
Target IP address: 20.202.255.251
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 60.0.27.252
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.202.255.251, timeout is 2 seconds:
Packet sent with a source address of 60.0.27.252
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/115/180 ms
RC3_2#
RC3_2#ping
Protocol [ip]:
Target IP address: 30.1.255.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 60.0.27.252
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 30.1.255.1, timeout is 2 seconds:
Packet sent with a source address of 60.0.27.252
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/106/132 ms
RC3_2#ping
Protocol [ip]:
Target IP address: 40.0.3.251
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 60.0.27.252
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 40.0.3.251, timeout is 2 seconds:
Packet sent with a source address of 60.0.27.252
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 168/190/220 ms

```

e)

Sim. Todas as tabelas de encaminhamento de routers que correm BGP vão incluir todas as redes (incluindo as 4.4.4.4 e 8.8.8.8) exceto as redes que usam endereçamento privado no AS do ISP.

f)

Os routers P não conseguem fazer *ping* a endereços noutros AS porque estes routers não participam no BGP. E também porque sendo routers internos que usam endereçamento privado, numa resposta ao *ping* enviado, o endereço de destino não iria conhecer a origem.

g)

Faz sentido usar endereços privados dentro do AS apenas se não quisermos que outros ASs comuniquem com este e que estes endereços não sejam conhecidos pela Internet. Entre ASs não faz sentido.

h)

Para verificar a rota que o PE7 toma até à Internet simulada por 4.4.4.4 foi efetuado um *ping* estendido em modo Record. Podemos ver o resultado de um pacote abaixo.

```
Reply to request 4 (232 ms). Received packet has options
Total option bytes= 40, padded length=40
Record route:
(10.3.245.2)
(10.1.44.1)
(10.1.38.2)
(10.1.28.2)
(10.1.23.2)
(10.1.17.2)
(20.201.12.2)
(11.101.4.2)
(4.4.4.4)
<*>
End of list
```

Figura 36 - Resultado ping entre PE7 e Internet

A rota tomada não traz qualquer surpresa, podia ter saído do AS 302 pelo router PE3 mas faz mais sentido pelo PE1 pois tem uma rota mais direta a 4.4.4.4.

i)

Para verificar que rotas o tráfego interno do Cliente 2 toma até à Internet, simulada por 4.4.4.4, foi feito um *traceroute* no router RC2_2 para o endereço 4.4.4.4.

```
RC2_2#traceroute 4.4.4.4
Type escape sequence to abort.
Tracing the route to 4.4.4.4
 0 10.0.50.1 64 msec 60 msec 60 msec
 1 10.0.49.1 60 msec 88 msec 56 msec
 2 10.3.245.1 88 msec 92 msec 104 msec
 3 10.1.44.2 116 msec 124 msec 120 msec
 4 10.1.38.1 148 msec 120 msec 120 msec
 5 10.1.28.1 148 msec 180 msec 168 msec
 6 10.1.23.1 180 msec 176 msec 176 msec
 7 10.1.17.1 204 msec 212 msec 208 msec
```

Figura 37 - Resultado do *traceroute*

j)

A rota usada entre o PC101_1 e o router R102_2 é a apresentada abaixo. A figura mostra o *traceroute* entre a origem e o destino que passam pela rota N2 e N3.

```
R101_1#traceroute 11.102.3.252
Type escape sequence to abort.
Tracing the route to 11.102.3.252

 1 11.101.2.2 56 msec 28 msec 44 msec
 2 10.102.3.2 20 msec 48 msec 40 msec
```

Figura 38 - Resultado do *traceroute*

k)

A rota usada entre o PC101_1 e o router R102_2 é a apresentada abaixo. A figura mostra o *traceroute* entre a origem e o destino que passam pela rota N2, N3 e N7.

```
R101_1#traceroute 20.202.255.253
Type escape sequence to abort.
Tracing the route to 20.202.255.253

 1 11.101.2.2 24 msec 44 msec 8 msec
 2 10.102.3.2 88 msec 40 msec 48 msec
 3 11.102.7.2 108 msec 100 msec 76 msec
```

Figura 39 - Resultado do *traceroute*

l)

O router R202_1 vai utilizar a rota diretamente conectada a R202_3, a N11.

m)

O router R201_1 faz *advertising* da *subnet* 20.201.0.0/20, logo se algum router quiser enviar pacotes para um endereço dessa gama vai ser o R201_1 a tratar disso. Porém este router só tem alguns endereços na sua tabela de encaminhamento logo se ele receber um endereço que não conheça pode vir a causar problemas de *looping* (pode enviar de volta o pacote recebido e ficar “preso”). Logo criar uma rota estática para Null0 trata desse problema de *looping* que possa vir a acontecer (o tráfego será descartado no R201_10).

n)

Faz mais sentido utilizar como endereço IP de um vizinho (*neighbor*) iBGP o endereço da interface de *Loopback0* utilizada como router ID nesse vizinho. Esta configuração já é a atual não sendo necessário mudar.

o)

O comando **update-source** indica ao dispositivo em questão que deve comunicar com o vizinho apresentada pela interface indicada neste comando. Nos casos da nossa topologia a interface indicada é o *Loopback0* que faz sentido de acordo com o que decidimos, comunicação pelo *Loopback0* caso alguma falha física. O comando **next-hop-self** indica que em qualquer *update* recebido para o vizinho em questão a *next-hop* será o router em questão. Todos os comandos utilizados foram configurados corretamente.

p)

No AS 102 não é necessário fazer a redistribuição das *subnets* BGP no OSPF pois é efetuado o comando **no synchronization** na configuração do BGP. E também porque todos os routers desse AS configuram tanto BGP como OSPF. No AS 202 todos os routers configuram o BGP e o OSPF e há redistribuição das rotas BGP no processo 202 OSPF, isto é necessário devido aos vizinhos diferentes que cada router possui – criando assim uma ligação entre todos os routers para que possa alongar os caminhos para o tráfego.

q)

No ISP existem routers que não “falam” BGP e por isso os routers que usam BGP têm de providenciar essas rotas BGP aos routers que não o conhecem para que não criem problemas de looping nos encaminhamentos. Para resolver este problema faz-se a redistribuição das rotas BGP no protocolo interno, o OSPF. Se isso não se fizer, os routers vão continuar à espera antes de usarem qualquer rota anunciada por iBGP. Mas no caso do ISP essa redistribuição é feita logo não é preciso usar o comando **no synchronization** que diria aos routers para não esperar.

Já foram mostrados anteriormente vários *pings* a demonstrar uma boa comunicação entre os dispositivos. Abaixo estão apresentadas as tabelas de encaminhamento de cada router fronteira de cada AS pedido no enunciado.

```
R101 R1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

  4.0.0.0/32 is subnetted, 1 subnets
    C 4.4.4.4 is directly connected, Loopback0
  20.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
    B 20.201.0.0/20 [20/0] via 11.101.4.2, 05:13:03
    B 20.202.0.0/16 [20/0] via 11.101.2.2, 05:12:51
  194.14.59.0/32 is subnetted, 1 subnets
    B 194.14.59.251 [20/0] via 11.101.4.2, 05:11:18
  8.0.0.0/32 is subnetted, 1 subnets
    B 8.8.8.8 [20/0] via 11.101.2.2, 05:12:51
  40.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
    B 40.0.0.0/22 [20/0] via 11.101.2.2, 05:11:48
    B 40.0.3.251/32 [20/0] via 11.101.2.2, 05:11:48
    B 40.0.3.252/32 [20/0] via 11.101.2.2, 05:11:48
  11.0.0.0/8 is variably subnetted, 6 subnets, 5 masks
    C 11.101.4.0/30 is directly connected, GigabitEthernet5/0
    C 11.101.2.0/30 is directly connected, GigabitEthernet2/0
    B 11.102.0.0/22 [20/1] via 11.101.2.2, 05:13:11
    S 11.101.0.0/21 is directly connected, Null0
    C 11.101.1.0/24 is directly connected, FastEthernet0/0
    C 11.101.7.251/32 is directly connected, Loopback0
  60.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
    B 60.0.26.0/23 [20/0] via 11.101.4.2, 05:12:28
    B 60.0.0.0/19 [20/0] via 11.101.4.2, 05:12:28
  30.0.0.0/14 is subnetted, 1 subnets
    B 30.0.0.0 [20/0] via 11.101.4.2, 05:12:29
  194.14.56.0/23 [20/0] via 11.101.4.2, 05:11:20
```

Figura 41 - Tabela de routing AS 101

```
R301 R1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

  4.0.0.0/32 is subnetted, 1 subnets
    C 4.4.4.4 [20/0] via 30.1.254.132, 05:14:57
  20.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
    B 20.201.0.0/20 [20/0] via 30.1.254.132, 05:14:57
    B 20.202.0.0/16 [20/0] via 30.1.254.132, 05:14:57
  194.14.59.0/32 is subnetted, 1 subnets
    C 194.14.59.251 is directly connected, Loopback0
  8.0.0.0/32 is subnetted, 1 subnets
    B 8.8.8.8 [20/0] via 30.1.254.132, 05:14:57
  40.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
    B 40.0.0.0/22 [20/1] via 30.1.254.133, 05:14:57
    B 40.0.3.251/32 [20/11] via 30.1.254.133, 05:14:57
    B 40.0.3.252/32 [20/0] via 30.1.254.133, 05:14:57
  11.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
    B 11.102.0.0/22 [20/0] via 30.1.254.132, 05:14:58
    B 11.101.0.0/21 [20/0] via 30.1.254.132, 05:14:58
  60.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
    B 60.0.26.0/23 [20/0] via 30.1.254.132, 05:14:58
    B 60.0.0.0/19 [20/0] via 30.1.212.2, 05:14:58
  30.0.0.0/8 is variably subnetted, 3 subnets, 3 masks
    B 30.0.0.0/14 [20/0] via 30.1.212.2, 05:14:58
    C 30.1.254.128/25 is directly connected, FastEthernet1/1
    C 30.1.212.0/30 is directly connected, GigabitEthernet2/0
  194.14.56.0/23 is directly connected, FastEthernet0/0
```

Figura 40 - Tabela de routing AS 301

Como podemos verificar os routers apresentam as rotas que têm configuradas diretamente (C) e as rotas que aprendem pelo BGP, seja eBGP ou iBGP. Os routers que pertencem a ASs que utilizam protocolos internos contêm rotas nas suas tabelas que foram conhecidas através desse protocolo – através dos seus vizinhos, neste caso sendo o protocolo OSPF.

```

RC3_1#SH IP ROUTE
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

 4.0.0.0/32 is subnetted, 1 subnets
B   4.4.4.4 [20/0] via 10.1.29.1, 05:18:27
B   20.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
    B   20.201.0.0/20 [20/0] via 10.1.29.1, 05:18:27
    B   20.202.0.0/16 [20/0] via 10.1.29.1, 05:18:27
B   194.14.59.0/32 is subnetted, 1 subnets
    B   194.14.59.251 [20/0] via 10.1.29.1, 05:17:56
B   8.0.0.0/32 is subnetted, 1 subnets
    B   8.8.8.8 [20/0] via 10.1.29.1, 05:18:27
B   40.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
    B   40.0.0.0/22 [20/0] via 10.1.29.1, 05:17:56
    B   40.0.3.251/32 [20/0] via 10.1.29.1, 05:17:56
    B   40.0.3.252/32 [20/0] via 10.1.29.1, 05:17:56
B   10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
    C   10.1.29.0/26 is directly connected, FastEthernet1/0
    C   10.0.39.0/30 is directly connected, FastEthernet1/1
B   11.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
    B   11.102.0.0/22 [20/0] via 10.1.29.1, 05:18:27
    B   11.101.0.0/21 [20/0] via 10.1.29.1, 05:18:28
B   60.0.0.0/8 is variably subnetted, 5 subnets, 4 masks
    C   60.0.26.0/24 is directly connected, FastEthernet0/0
    O E2 60.0.26.0/23 [110/1] via 10.0.39.2, 05:18:19, FastEthernet1/1
    B   60.0.0.0/10 [20/1] via 10.1.29.1, 05:18:51
    O   60.0.27.252/32 [110/11] via 10.0.39.2, 05:18:19, FastEthernet1/1
    C   60.0.27.251/32 is directly connected, Loopback0
B   30.0.0.0/14 is subnetted, 1 subnets
    B   30.0.0.0 [20/1] via 10.1.29.1, 05:18:51
B   194.14.56.0/23 [20/0] via 10.1.29.1, 05:17:57

```

Figura 42 - Tabela de *routing* Cliente 3

```

PE1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

 4.0.0.0/32 is subnetted, 1 subnets
B   4.4.4.4 [20/0] via 20.201.12.1, 05:20:56
B   20.0.0.0/8 is variably subnetted, 4 subnets, 3 masks
    C   20.202.131.0/30 is directly connected, GigabitEthernet5/0
    C   20.201.12.0/30 is directly connected, GigabitEthernet2/0
    B   20.201.0.0/20 [20/0] via 20.201.12.1, 05:20:56
    B   20.202.0.0/16 [20/0] via 20.202.131.1, 05:20:56
B   194.14.59.0/32 is subnetted, 1 subnets
    O E2 194.14.59.251 [110/1] via 10.1.17.2, 05:20:24, GigabitEthernet4/0
B   8.0.0.0/32 is subnetted, 1 subnets
    B   8.8.8.8 [20/0] via 20.202.131.1, 05:20:56
B   40.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
    O E2 40.0.0.0/22 [110/1] via 10.1.17.2, 05:20:19, GigabitEthernet4/0
    O E2 40.0.3.251/32 [110/1] via 10.1.17.2, 05:20:20, GigabitEthernet4/0
    O E2 40.0.3.252/32 [110/1] via 10.1.17.2, 05:20:20, GigabitEthernet4/0
B   10.0.0.0/8 is variably subnetted, 27 subnets, 3 masks
    O IA 10.0.26.0/30 [110/13] via 10.1.20.2, 05:21:33, GigabitEthernet3/0
    O IA 10.0.27.0/30 [110/14] via 10.1.20.2, 05:21:33, GigabitEthernet3/0
    O   10.1.25.0/30 [110/25] via 10.1.17.2, 05:21:34, GigabitEthernet4/0
    O   10.1.29.0/26 [110/125] via 10.1.17.2, 05:21:34, GigabitEthernet4/0
    O   10.1.28.0/30 [110/25] via 10.1.17.2, 05:21:34, GigabitEthernet4/0
    C   10.1.19.0/30 is directly connected, FastEthernet1/0
    C   10.1.17.0/30 is directly connected, GigabitEthernet4/0
    O   10.1.23.0/30 [110/15] via 10.1.17.2, 05:21:34, GigabitEthernet4/0
    O   10.1.22.0/30 [110/35] via 10.1.17.2, 05:21:35, GigabitEthernet4/0
    C   10.1.20.0/30 is directly connected, GigabitEthernet3/0
    O IA 10.0.42.0/30 [110/24] via 10.1.20.2, 05:21:35, GigabitEthernet3/0
    O   10.1.41.0/30 [110/45] via 10.1.17.2, 05:21:35, GigabitEthernet4/0
    O   10.1.44.0/30 [110/37] via 10.1.17.2, 05:21:35, GigabitEthernet4/0
    O IA 10.0.35.0/30 [110/16] via 10.1.20.2, 05:21:34, GigabitEthernet3/0
    O   10.1.38.0/30 [110/35] via 10.1.17.2, 05:21:36, GigabitEthernet4/0
    O   10.1.36.0/30 [110/35] via 10.1.17.2, 05:21:36, GigabitEthernet4/0
    O E2 10.0.50.0/30 [110/20] via 10.1.20.2, 05:21:26, GigabitEthernet3/0
    O E2 10.0.49.0/30 [110/20] via 10.1.20.2, 05:21:26, GigabitEthernet3/0
    O IA 10.3.145.0/30 [110/124] via 10.1.20.2, 05:21:36, GigabitEthernet3/0
    O IA 10.0.255.4/32 [110/15] via 10.1.20.2, 05:21:35, GigabitEthernet3/0
    O IA 10.0.255.6/32 [110/25] via 10.1.20.2, 05:21:37, GigabitEthernet3/0
    O IA 10.0.255.1/32 [110/11] via 10.1.20.2, 05:21:36, GigabitEthernet3/0
    O IA 10.0.255.3/32 [110/14] via 10.1.20.2, 05:21:36, GigabitEthernet3/0
    O IA 10.0.255.2/32 [110/14] via 10.1.20.2, 05:21:52, GigabitEthernet3/0
    O IA 10.0.242.0/30 [110/13] via 10.1.20.2, 05:21:52, GigabitEthernet3/0
    O IA 10.0.241.0/30 [110/13] via 10.1.20.2, 05:21:52, GigabitEthernet3/0
    O IA 10.3.245.0/30 [110/34] via 10.1.20.2, 05:21:53, GigabitEthernet3/0
B   11.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
    B   11.102.0.0/22 [20/0] via 20.201.12.1, 05:21:17
    B   11.101.0.0/21 [20/0] via 20.201.12.1, 05:21:17
B   60.0.0.0/8 is variably subnetted, 6 subnets, 5 masks
    O E2 60.0.28.0/24 [110/20] via 10.1.20.2, 05:21:44, GigabitEthernet3/0
    B   60.0.26.0/23 [200/0] via 30.1.255.4, 05:20:47
    O E2 60.0.0.0/19 [110/1] via 10.1.17.2, 05:21:44, GigabitEthernet4/0
    O E2 60.0.31.128/25 [110/20] via 10.1.20.2, 05:21:44, GigabitEthernet3/0

```

Figura 43 (Incompleta) - Tabela de routing AS 302

2 – Implementação de políticas no iBGP no ISP

a)

No caso de não existirem filtros ativos numa sessão BGP o router irá escolher o caminho para anunciar/receber as suas rotas. A sua escolha baseia-se no menor número de ASs, ou seja, o caminho escolhido será aquele que passe pelo menor número de ASs, por um lado esta medida é positiva, uma vez que o caminho escolhido tende a ser o mais rápido, mas também pode ser prejudicial, uma vez que poderá causar tráfego excessivo ou indesejado, numa AS.

b)

Os valores *default* dos timers hold e keepalive, respetivamente, são 180 e 60 segundos. Podemos verificar isso com o comando **sh bgp neighbors**.

```
PE1#sh bgp neighbors
BGP neighbor is 20.201.12.1, remote AS 201, external link
  BGP version 4, remote router ID 20.201.15.251
  BGP state = Established, up for 09:34:45
  Last read 00:00:53, last write 00:00:45, hold time is 180, keepalive interval is 60 seconds
```

Figura 44 - Vizinho BGP do router PE1

A razão do tempo ser tão longo é devido ao *hold-down* timer ser o triplo do timer *keepalive*, ou seja, as mensagens *keepalive* são enviadas a cada terço do *hold timer*.

c)

Se se ajustasse em todas as sessões iBGP um *keepalive* de 5 e um *hold* de 15, então a cada 5 segundos é enviada uma mensagem de *keepalive* a todos os *peers* e que passado 15 segundos sem receber um *keepalive* um *peer* BGP é considerado *dead*. Num ambiente controlado e estável esta mudança pode ser bastante eficaz para reduzir tempos de espera nas ligações BGP mas noutro caso, num ambiente real, pode causar distúrbios nas tabelas devido às mudanças constantes.

d)

Para que as mensagens iBGP possam continuar a chegar a esse router mesmo se falhar qualquer interface, implementa-se o comando **neighbor update-source Loopback0** que indica que o router tem de comunicar com esse vizinho pela interface *Loopback0* – é a melhor maneira de assegurar a ligação.

3 – Políticas de eBGP, entre o ISP e os seus clientes

Os routers do AS 302 que têm como vizinhos BGP os clientes do ISP são o router PE6 que comunica com o AS 301, Cliente 4 e os routers PE4 e PE5 que comunicam com o Cliente 3. O router PE2 comunica com os dois clientes através do IXP.

- O ISP origina sempre a rota *default* para os seus clientes.
 - Para originar a rota *default* para cada cliente, em cada router deve-se implementar o comando **neighbor <ip-address> default-originate**.
- Aceitar um máximo de 50 prefixos
 - Para isto executa-se o comando **maximum-prefix 50** em cada neighbor do router.
- Aceitar apenas tráfego das redes que lhes delegou ou que eles possuem oficialmente
 - Para isto é necessário criar uma **prefix-list** que permite os prefixos 30.0.0.0/14 e 60.0.0.0/19 – que são os que o ISP delega e uma outra lista que permita o prefixo que o cliente possui.
- Garantir que apenas anuncia a rota *default*
 - Criar uma **prefix-list** que permita a rota *default* – 0.0.0.0/0 com o comando **ip prefix-list <name> permit|deny <prefix>**.

Estas mudanças são apresentadas abaixo nos routers do ISP indicados acima.

```
neighbor 30.1.212.1 activate
neighbor 30.1.212.1 default-originate
neighbor 30.1.212.1 remove-private-as
neighbor 30.1.212.1 prefix-list ACCEPT-ROUTES in
neighbor 30.1.212.1 prefix-list SEND-DEFAULT out
neighbor 30.1.212.1 maximum-prefix 50
```

Figura 46 - Configuração do cliente vizinho no router PE6

```
ip prefix-list ACCEPT-ROUTES seq 5 permit 30.0.0.0/14
ip prefix-list ACCEPT-ROUTES seq 10 permit 60.0.0.0/19
ip prefix-list ACCEPT-ROUTES seq 15 permit 194.14.56.0/22
!
ip prefix-list SEND-DEFAULT seq 5 permit 0.0.0.0/0
```

Figura 45 - Criação das listas de prefixos para o Cliente 4 no PE6

```
neighbor 10.1.29.4 activate
neighbor 10.1.29.4 default-originate
neighbor 10.1.29.4 prefix-list ACCEPT-ROUTES in
neighbor 10.1.29.4 prefix-list SEND-DEFAULT out
neighbor 10.1.29.4 maximum-prefix 50
neighbor 10.1.29.5 activate
neighbor 10.1.29.5 default-originate
neighbor 10.1.29.5 prefix-list ACCEPT-ROUTES in
neighbor 10.1.29.5 prefix-list SEND-DEFAULT out
neighbor 10.1.29.5 maximum-prefix 50
```

Figura 47 - Configuração do cliente vizinho no router PE4/PE5

```
ip prefix-list ACCEPT-ROUTES seq 5 permit 30.0.0.0/14
ip prefix-list ACCEPT-ROUTES seq 10 permit 60.0.0.0/19
ip prefix-list ACCEPT-ROUTES seq 15 permit 60.0.26.0/23
!
ip prefix-list SEND-DEFAULT seq 5 permit 0.0.0.0/0
```

Figura 48 - Criação das listas de prefixos para o Cliente 4 no PE4/PE5

A configuração dos vizinhos no PE4 e no PE5 é idêntica pois ambos contém as mesmas ligações para o AS 65005.

a)

Neste momento não existe BGP no cliente 2. Para configurar eBGP seria necessário configurá-lo no router RC2_1 do cliente 2 e no router do ISP que está diretamente ligado a este cliente, o PE7.

Para o PE7:

```
router bgp 302
bgp-log-neighbor-changes
network 30.0.0.0 mask 255.252.0.0
network 60.0.0.0 mask 255.255.224.0
neighbor 10.3.245.1 remote-as 302
neighbor 10.3.245.1 update-source Loopback0
neighbor 60.0.29.152 remote-as 2
neighbor 60.0.29.152 update-source Loopback0
neighbor 60.0.29.152 maximum-prefix 50
no synchronization
```

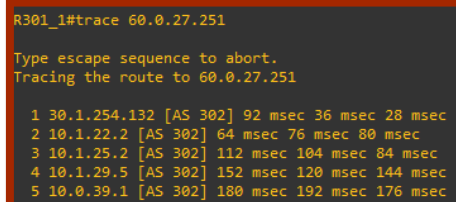
No OSPF 302 fazer redistribuição de BGP.

Para o RC2_1:

```
router bgp 2
bgp-log-neighbor-changes
neighbor 10.9.49.1 remote-as 302
neighbor 10.0.49.1 update-source Loopback0
neighbor 60.0.29.152 remote-as 2
neighbor 60.0.29.152 update-source Loopback0
no synchronization
```

No RIP fazer redistribuição de BGP.

b)



```
R301_1#trace 60.0.27.251
Type escape sequence to abort.
Tracing the route to 60.0.27.251

 1 30.1.254.132 [AS 302] 92 msec 36 msec 28 msec
 2 10.1.22.2 [AS 302] 64 msec 76 msec 80 msec
 3 10.1.25.2 [AS 302] 112 msec 104 msec 84 msec
 4 10.1.29.5 [AS 302] 152 msec 120 msec 144 msec
 5 10.0.39.1 [AS 302] 180 msec 192 msec 176 msec
```

Figura 49 - Resultado de trace entre R301_1 e RC3_1

A rota usada é a descrita acima.

c)

Sim.

d)

Num ISP real um número elevado de ligações entre este e outros ISPs poderia causar maior tráfego o que poderia, em consequência, criar mais congestionamento e

desacelerar o processo de transmissão de pacotes. Outro aspeto é o consumo de recursos que é algo desnecessário se existem outras maneiras de criar uma comunicação efetiva entre ASs.

4 – Route Refletor (RR)

Para criar um *route reflector* primeiro é necessário que existe *full-mesh* na topologia. Full-mesh é quando todos os routers estão todos ligados uns aos outros por meio duma ligação física.

A função deste *route reflector* é mesmo para reduzir o tamanho da *mesh*. Este reflector vai distribuir as rotas aprendidas para os outros vizinhos interiores BGP.

```
P4#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

 4.0.0.0/32 is subnetted, 1 subnets
O E2  4.4.4.4 [110/1] via 10.1.36.2, 00:30:29, GigabitEthernet3/0
 20.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
O E2  20.201.0.0/20 [110/1] via 10.1.36.2, 00:30:29, GigabitEthernet3/0
O E2  20.202.0.0/16 [110/1] via 10.1.36.2, 00:30:29, GigabitEthernet3/0
194.14.59.0/32 is subnetted, 1 subnets
O E2  194.14.59.251 [110/1] via 10.1.36.2, 00:30:29, GigabitEthernet3/0
 8.0.0.0/32 is subnetted, 1 subnets
O E2  8.8.8.8 [110/1] via 10.1.36.2, 00:30:29, GigabitEthernet3/0
40.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
O E2  40.0.0.0/22 [110/1] via 10.1.36.2, 00:30:29, GigabitEthernet3/0
O E2  40.0.3.251/32 [110/1] via 10.1.36.2, 00:30:29, GigabitEthernet3/0
O E2  40.0.3.252/32 [110/1] via 10.1.36.2, 00:30:29, GigabitEthernet3/0
10.0.0.0/8 is variably subnetted, 27 subnets, 3 masks
O    10.0.26.0/30 [110/6] via 10.0.35.1, 03:40:23, GigabitEthernet2/0
C    10.0.27.0/30 is directly connected, GigabitEthernet5/0
O    10.1.25.0/30 [110/30] via 10.1.36.2, 00:30:30, GigabitEthernet3/0
O    10.1.29.0/26 [110/110] via 10.1.36.2, 00:30:31, GigabitEthernet3/0
O    10.1.28.0/30 [110/20] via 10.1.36.2, 00:30:31, GigabitEthernet3/0
O    10.1.19.0/30 [110/130] via 10.1.36.2, 00:30:31, GigabitEthernet3/0
O    10.1.17.0/30 [110/35] via 10.1.36.2, 00:30:31, GigabitEthernet3/0
O    10.1.23.0/30 [110/30] via 10.1.36.2, 00:30:31, GigabitEthernet3/0
O    10.1.22.0/30 [110/40] via 10.1.36.2, 00:30:31, GigabitEthernet3/0
O    10.1.20.0/30 [110/45] via 10.1.36.2, 00:30:31, GigabitEthernet3/0
C    10.0.42.0/30 is directly connected, GigabitEthernet4/0
O    10.1.41.0/30 [110/30] via 10.1.36.2, 00:30:31, GigabitEthernet3/0
O    10.1.44.0/30 [110/22] via 10.1.36.2, 00:30:31, GigabitEthernet3/0
C    10.0.35.0/30 is directly connected, GigabitEthernet2/0
O    10.1.38.0/30 [110/20] via 10.1.36.2, 00:30:31, GigabitEthernet3/0
C    10.1.36.0/30 is directly connected, GigabitEthernet3/0
O E2  10.0.50.0/30 [110/20] via 10.0.42.2, 00:30:31, GigabitEthernet4/0
O E2  10.0.49.0/30 [110/20] via 10.0.42.2, 00:30:31, GigabitEthernet4/0
O IA  10.3.145.0/30 [110/110] via 10.0.42.2, 00:30:31, GigabitEthernet4/0
C    10.0.255.4/32 is directly connected, Loopback0
O    10.0.255.6/32 [110/11] via 10.0.42.2, 03:40:23, GigabitEthernet4/0
O    10.0.255.1/32 [110/5] via 10.0.27.1, 03:40:23, GigabitEthernet5/0
O    10.0.255.3/32 [110/4] via 10.0.35.1, 03:40:23, GigabitEthernet2/0
O    10.0.255.2/32 [110/4] via 10.0.27.1, 03:40:23, GigabitEthernet5/0
O    10.0.242.0/30 [110/4] via 10.0.27.1, 03:40:23, GigabitEthernet5/0
O    10.0.241.0/30 [110/4] via 10.0.27.1, 03:40:23, GigabitEthernet5/0
O IA  10.3.245.0/30 [110/20] via 10.0.42.2, 00:30:31, GigabitEthernet4/0
11.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
O E2  11.102.0.0/22 [110/1] via 10.1.36.2, 00:30:31, GigabitEthernet3/0
O E2  11.101.0.0/21 [110/1] via 10.1.36.2, 00:30:31, GigabitEthernet3/0
60.0.0.0/8 is variably subnetted, 5 subnets, 4 masks
O E2  60.0.28.0/24 [110/20] via 10.0.42.2, 00:30:31, GigabitEthernet4/0
O E2  60.0.0.0/19 [110/1] via 10.1.36.2, 00:30:31, GigabitEthernet3/0
O E2  60.0.31.128/25 [110/20] via 10.0.42.2, 00:30:31, GigabitEthernet4/0
O E2  60.0.29.251/32 [110/20] via 10.0.42.2, 00:30:32, GigabitEthernet4/0
--More--
```

Figura 50 - sh ip route P4

Fase 4 – BGPv4 avançado

1 - Ligações eBGP de trânsito e *peering* do ISP

No router PE2 já existe uma relação de *peering* com o AS 303, o Cliente 4 (através do IXP). As alterações feitas, filtros aplicados, na configuração foram as seguintes.

```
PE2(config)#router bgp 302
PE2(config-router)#ex
PE2(config)#ip prefix-list PERMIT-LIST permit 30.0.0.0/14
PE2(config)#ip prefix-list PERMIT-LIST permit 60.0.0.0/19
PE2(config)#router bgp 302
PE2(config-router)#neighbor 30.1.254.133 prefix-list PERMIT-LIST in
```

Figura 51 - Criação de **prefix-list** e aplicação da mesma

A configuração até agora apresentada das relações eBGP entre o AS 302 e o AS 301 são as corretas para o bom funcionamento e comunicação entre todos os routers presentes nesta rede.

```
router bgp 301
no synchronization
bgp log-neighbor-changes
network 194.14.56.0 mask 255.255.254.0
network 194.14.59.251 mask 255.255.255.255
neighbor 30.1.212.2 remote-as 302
neighbor 30.1.254.132 remote-as 302
neighbor 30.1.254.133 remote-as 303
no auto-summary
```

Figura 52 - BGP 301

A configuração abaixo referente ao router R202_1 é a corrente na topologia e estabelece a sessão BGP do AS 202, e que vai criar uma sessão de *peering* com o router PE1 do ISP.

```
router bgp 202
bgp log-neighbor-changes
neighbor 20.202.131.2 remote-as 302
neighbor 20.202.132.2 remote-as 302
neighbor 20.202.255.252 remote-as 202
neighbor 20.202.255.252 update-source Loopback0
neighbor 20.202.255.253 remote-as 202
neighbor 20.202.255.253 update-source Loopback0
!
address-family ipv4
neighbor 20.202.131.2 activate
neighbor 20.202.132.2 activate
neighbor 20.202.255.252 activate
neighbor 20.202.255.252 next-hop-self
neighbor 20.202.255.253 activate
neighbor 20.202.255.253 next-hop-self
no auto-summary
no synchronization
network 20.202.0.0 mask 255.255.0.0
exit-address-family
!
ip forward-protocol nd
ip route 20.202.0.0 255.255.0.0 Null0
```

Figura 53 - BGP 202 no R202_1

Como podemos verificar em cada router é identificado o outro como neighbor. As rotas

```
router bgp 302
bgp log-neighbor-changes
neighbor 20.201.12.1 remote-as 201
neighbor 20.202.131.1 remote-as 202
neighbor 30.1.255.2 remote-as 302
neighbor 30.1.255.2 update-source Loopback0
neighbor 30.1.255.3 remote-as 302
neighbor 30.1.255.3 update-source Loopback0
neighbor 30.1.255.4 remote-as 302
neighbor 30.1.255.4 update-source Loopback0
neighbor 30.1.255.5 remote-as 302
neighbor 30.1.255.5 update-source Loopback0
neighbor 30.1.255.6 remote-as 302
neighbor 30.1.255.6 update-source Loopback0
!
address-family ipv4
neighbor 20.201.12.1 activate
neighbor 20.201.12.1 remove-private-as
neighbor 20.202.131.1 activate
neighbor 20.202.131.1 remove-private-as
neighbor 30.1.255.2 activate
neighbor 30.1.255.2 next-hop-self
neighbor 30.1.255.3 activate
neighbor 30.1.255.3 next-hop-self
neighbor 30.1.255.4 activate
neighbor 30.1.255.4 next-hop-self
neighbor 30.1.255.5 activate
neighbor 30.1.255.5 next-hop-self
neighbor 30.1.255.6 activate
neighbor 30.1.255.6 next-hop-self
no auto-summary
no synchronization
network 30.0.0.0 mask 255.252.0.0
network 60.0.0.0 mask 255.255.224.0
exit-address-family
!
ip forward-protocol nd
ip route 30.0.0.0 255.252.0.0 Null0 250
ip route 60.0.0.0 255.255.224.0 Null0 250
```

Figura 54 - BGP 302 no PE1

estáticas identificadas são necessárias para essas rotas aparecerem na tabela e serem encaminhadas pelo BGP.

2 – Políticas de segurança do ISP relativas aos AS dos *tiers* superiores

Para evitar que os AS sejam de trânsito devem se criar *prefix-lists* que permitam apenas os prefixos que remetem a esse AS (e a dos seus clientes) e os vizinhos BGP devem receber apenas esses *prefix-lists*.

Para implementar as políticas indicadas usa-se o comando **route-map** que nos dá a possibilidade de criar restrições nos endereços que queremos receber/partilhar.

3 – Políticas de tráfego de saída do ISP

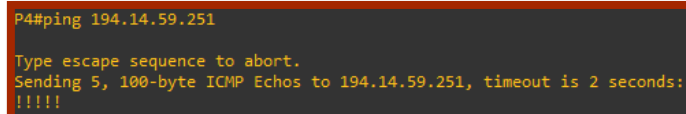
a)

Sim poder-se-ia realizar a agregação de endereços IPv4 nesta topologia, visto que o BGP disponibiliza esta opção usando *aggregate-address* com *summary-only*, mais corretamente seria também usado o atributo *as-set* na criação da agregação, assim quando é anunciado a agregação também é anunciado os AS agregados, sendo importante na detecção de *loops*, o BGP repara que tem o seu AS já na lista de agregação e descarta, prevenindo *loops*.

Fase 5

1 – Rotas internas no ISP

- a) Não vai existir nenhuma mudança pois o custo OSPF vai ser de 1 tanto para um cabo *FastEthernet* como para um *GigabitEthernet*.
- b) Não vai influenciar em nada pois este router já contém na sua tabela um caminho para o PE6.
- c) Sim. Para exemplo foi feito um *ping* entre o P4 e o router do AS 301.



```
P4#ping 194.14.59.251
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 194.14.59.251, timeout is 2 seconds:
!!!!
```

Figura 55 - Ping entre P4 e AS 301

- d) Para evitar esta redistribuição podia-se simplesmente configurar estes routers P com o protocolo BGP.
- e) Este comando serve para gerar uma rota *default* caso não haja o caminho na tabela e é necessário pois estes routers fazem fronteira com diferentes ASs.
- f) Na configuração OSPF nos routers PE1 e PE3 é feita a redistribuição das subnets aprendidas por BGP, ou seja, os routers internos que partilham o processo OSPF vão conhecer estes endereços aprendidos.

Conclusão

- Com este trabalho pudemos colocar em prática os conhecimentos e aprendizagens dados na cadeira de Redes de Internet até ao momento do trabalho, mais precisamente sobre o uso de BGP.

Webgrafia

- <https://smallbusiness.chron.com/advantages-disadvantages-using-private-ip-address-space-46424.html>
- <https://smallbusiness.chron.com/disadvantages-using-public-ip-addresses-69877.html>
- <https://www.techrepublic.com/forums/discussions/pros-cons-of-public-private-ips/>
- https://www.juniper.net/documentation/en_US/junos/topics/topic-map/ospf-areas.html
- <https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/networking/ospf/ospf-concepts/ospf-areas.html>
- <https://help.keenetic.com/hc/en-us/articles/213965789-What-is-the-difference-between-a-public-and-private-IP-address->
- <https://networklessons.com/ospf/ospf-lsa-types-explained>
- <https://networklessons.com/ospf/introduction-to-ospf-stub-areas>
- https://en.wikipedia.org/wiki/Default_route
- <https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/6208-nssa.html>
- <https://community.cisco.com/t5/switching/meaning-of-ping-response/td-p/1431049>
- <http://www.bgpexpert.com/nosync.php>
- https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/configuration/xr-3s/irg-xr-3s-book/irg-mvpn-safi.html